

Creating Your Information Security Incident Response Program



TEXAS DIR ISF 2017

Dave Gray

- Senior CyberSecurity Analyst –
 - Texas Comptroller of Public Accounts <http://comptroller.texas.gov>
 - Policy Author for Governance, Risk Management and Compliance (GRC)
- Board Member – ISSA Austin www.austinissa.org
- Instructor – Austin Community College (ACC) www.austincc.edu
 - CISSP CASP Prep Course
 - ITIL 2011 Foundation Exam Prep
- Retired Army – TXARNG Lieutenant Colonel
 - Managed IT Operations and Information Security for 5,000 users
 - Established one of the first CERTs for the Army National Guard
 - Military Pilot - AH1 Cobra, OH58 Kiowa, UH1 Huey
- Texas Instruments and Raytheon
 - Oracle DBA and Project Manager
- Certifications
 - CISSP, PMP, CAP, Security+, ITIL, CEH, EnCE, MCSE, MCSA
- www.linkedin.com/in/davidleegray



Information Security Incident Response



Information Security Incident Response Program



- Effective Incident Response capability improves incident detection, minimizes loss and destruction, mitigates exploited weaknesses and restores IT services
- Incident Response programs address governance, establish IR teams, emphasize training, and conduct self-assessment and evaluation

IR Program - Define

- Define Incident Response
- Establish Governance
- Identify Teams
- Initiate Training
- Self-Assessment



What is an Information Security Incident?

- An event which accidentally or deliberately results in unauthorized
 - Access,
 - Loss,
 - Disclosure,
 - Modification,
 - Disruption,
 - Destruction,
 - of Information or Information Resources



Information Security Incident (examples)

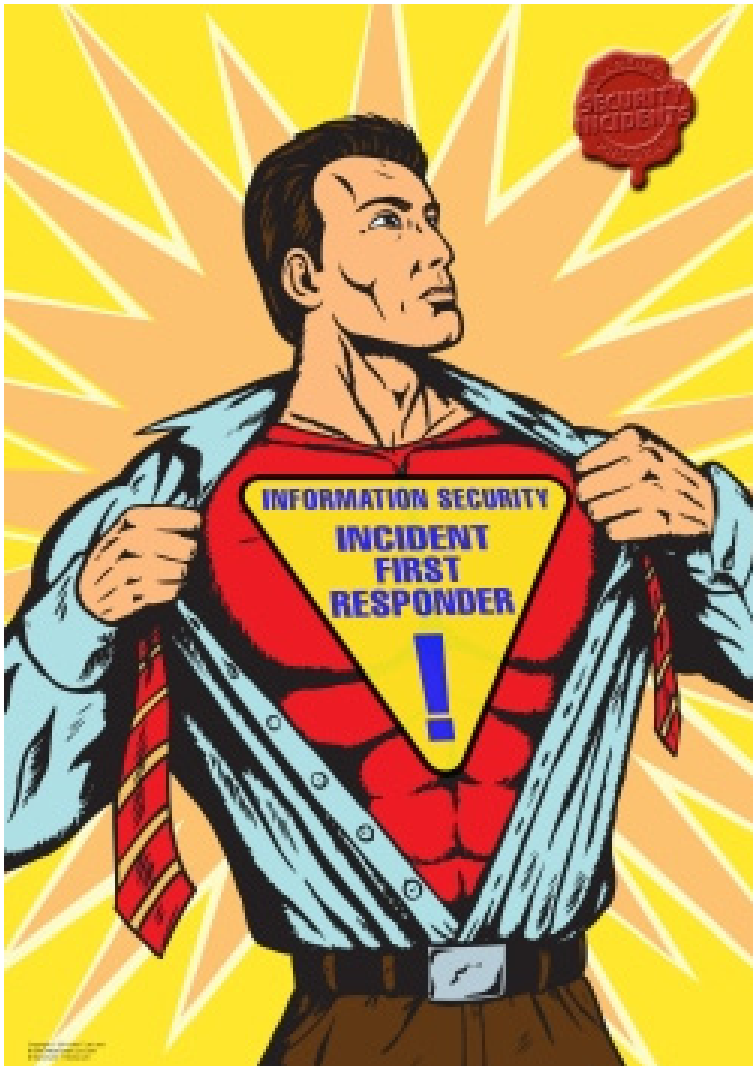
- Ransomware
- Business E-Mail Compromise (BEC)
- Denial-of-service attack (DDoS)
- Confidential data discovered on website
- Personally Identifying Information (PII) exposed
- Laptop / other media with PII is lost or stolen
- Data corruption by a virus or worm

What is Incident Response?

- Organized approach – to addressing and managing the aftermath of a security breach or attack (also known as an incident)
- Goal
 - Limit damage
 - Reduce recovery time and costs



Incident Response



- Incident Response
 - Prepares,
 - Detects,
 - Analyzes,
 - Contains,
 - Eradicates,
 - and Recovers
- From incident impact on
 - Confidentiality,
 - Integrity and
 - Availability of data.

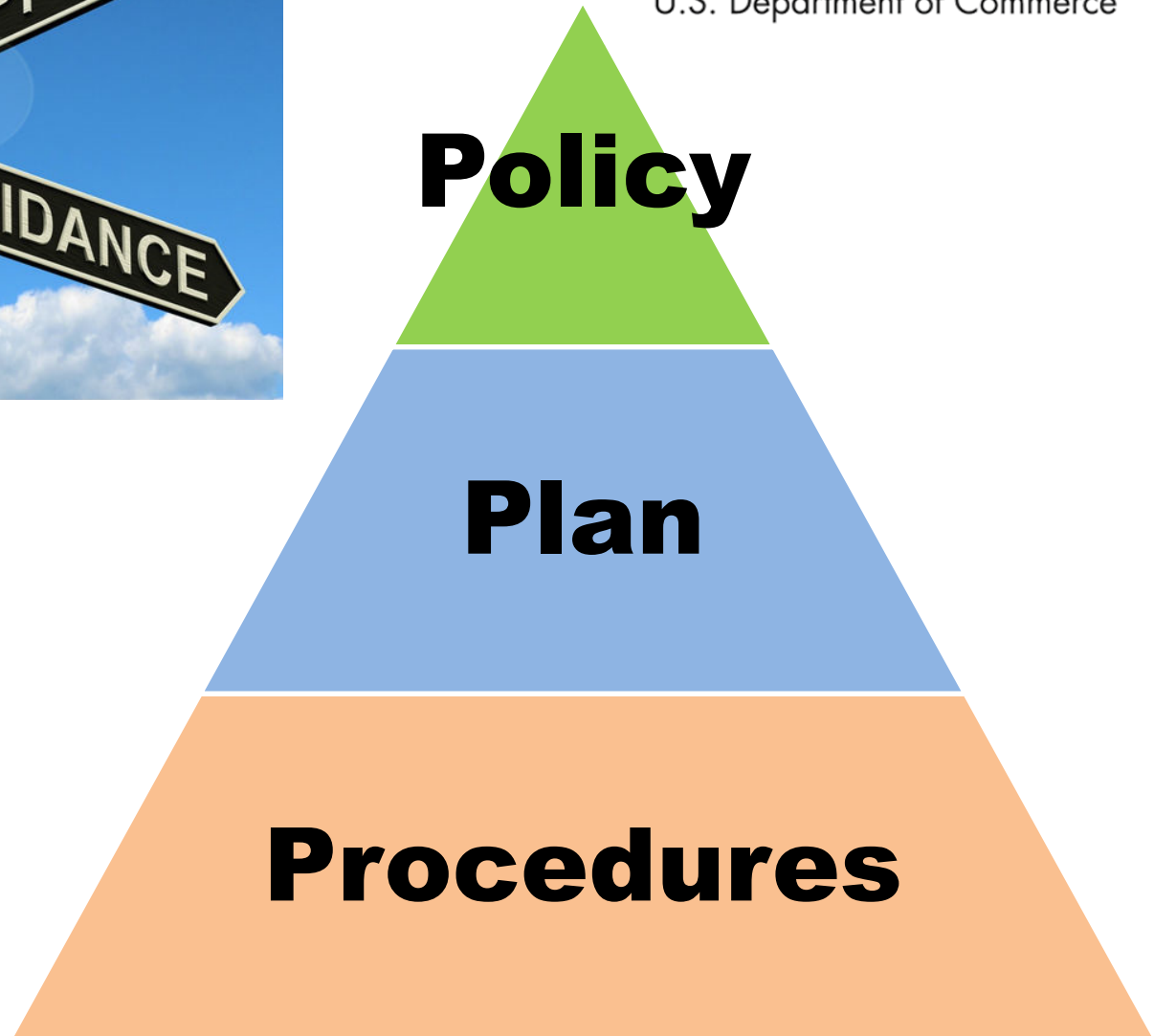
IR Program – Governance

- Define Incident Response
- **Establish Governance**
- Identify Teams
- Initiate Training
- Self-Assessment





NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



Access Documents During an Incident



**OneDrive
for Business**

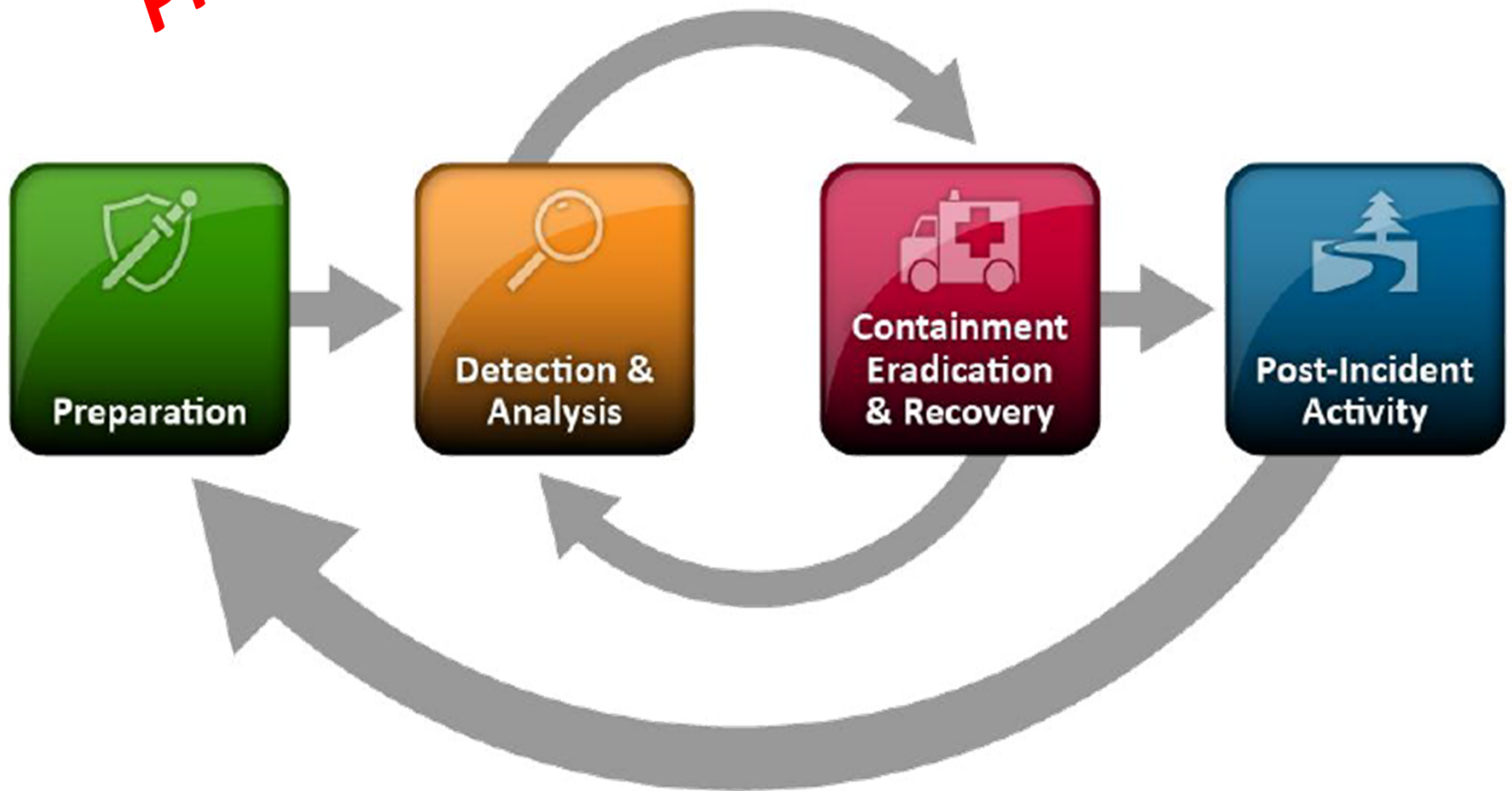


- Management Commitment
- Purpose and Objectives
- Scope
- Roles, Responsibilities
- Levels of Authority
- Prioritization/severity
- Performance metrics
- Reporting

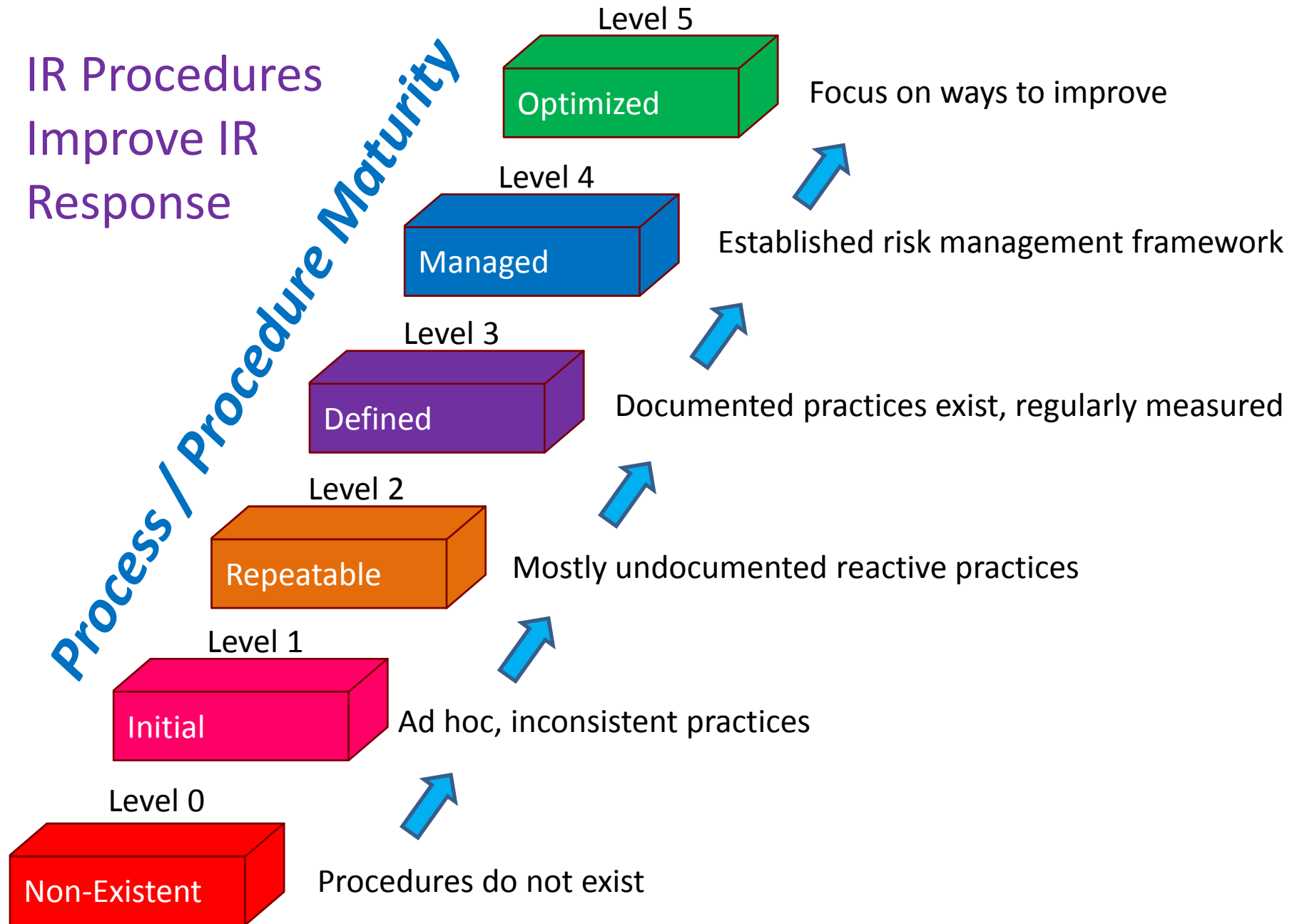
- Mission
- Strategies and goals
- Senior Mgmt Approval
- Organizational Approach
- Communication
- Metrics
- Roadmap for Maturing
- Program Integration



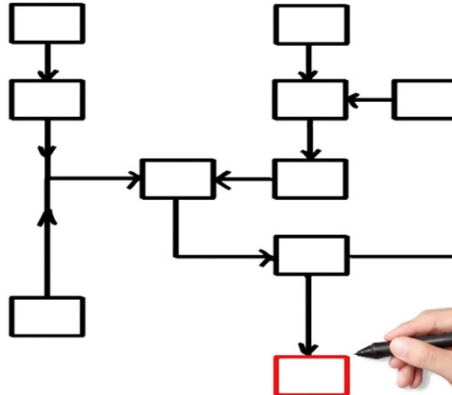
**Documenting
Processes**

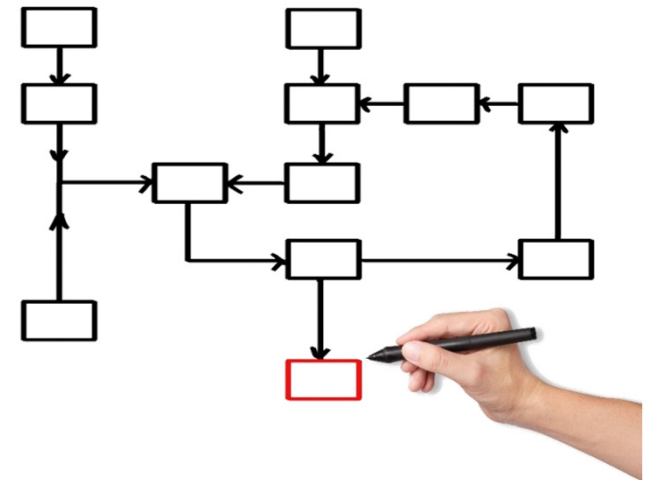


IR Procedures Improve IR Response



Written Procedures Mitigate Chaos
e.g. Notification Requirements

- Breach notification requirements are complex
 - Spelled out in Texas Statute
 - TX BCC Section 521.053
 - Multiple decision points –
 - Was data compromised? y/n
 - Data contains SPI? y/n
 - Data encrypted? y/n
 - Notification cost > \$250k ? y/n
 - # of individuals > 500k ? y/n
 - Contact information exists? y/n
 - Notification \$ may be covered by Cyber Insurance
- 



Written Procedures Mitigate Chaos

e.g. Notification Details

- What happened?
- When did it happen?
- When was it detected?
- How was it detected?
- What data was potentially compromised?
- How much data was compromised?
- Whose data was compromised?
- Why the recipient is being notified.
- What steps are/were being taken?
- What steps should individuals take?
- How to get additional information e.g. website, hotline, etc.



Written Procedures Mitigate Chaos

e.g. Prioritizing Incidents

- Priority 1 (CRITICAL)
 - 101 users or more are affected
- Priority 2 (HIGH)
 - 11 to 100 users are affected
- Priority 3 (MODERATE)
 - 2 to 10 users are affected
- Priority 4 (LOW)
 - A single user is affected

EXAMPLE

IR Program – Teams

- Define Incident Response
- Establish Governance
- **Identify Teams**
- Initiate Training
- Self-Assessment



IR Teams



- Management Team
- Technical Team
- Regulatory Contact Team
- Communications Team
- Contracting Team
- Criminal Investigation Team
- Ad Hoc Response Team
- External Support Team
- External Partners
- Communication Resources

Team Responsibilities

- Dependent on team functions such as
 - Communications
 - Notifying information owners of a compromise
 - Websites
 - Press Releases
 - Contracting
 - Facilitate vendor support
 - Establish contract retainers
 - Etc.



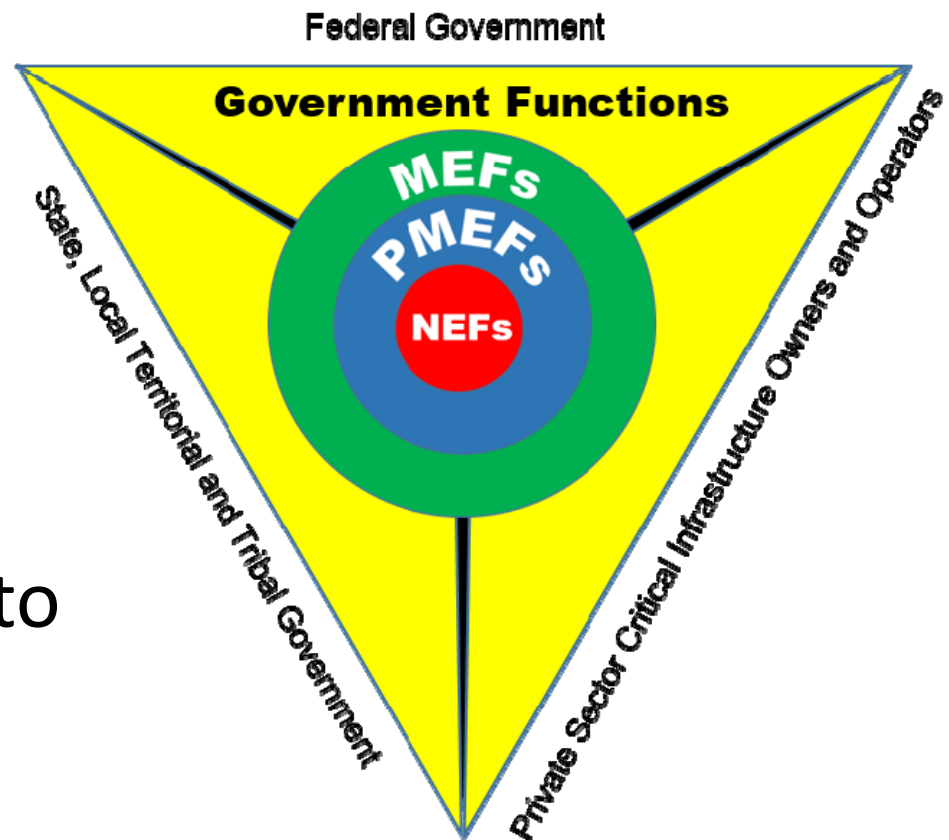
IR Program – Training

- Define Incident Response
- Establish Governance
- Identify Teams
- **Initiate Training**
- Self-Assessment

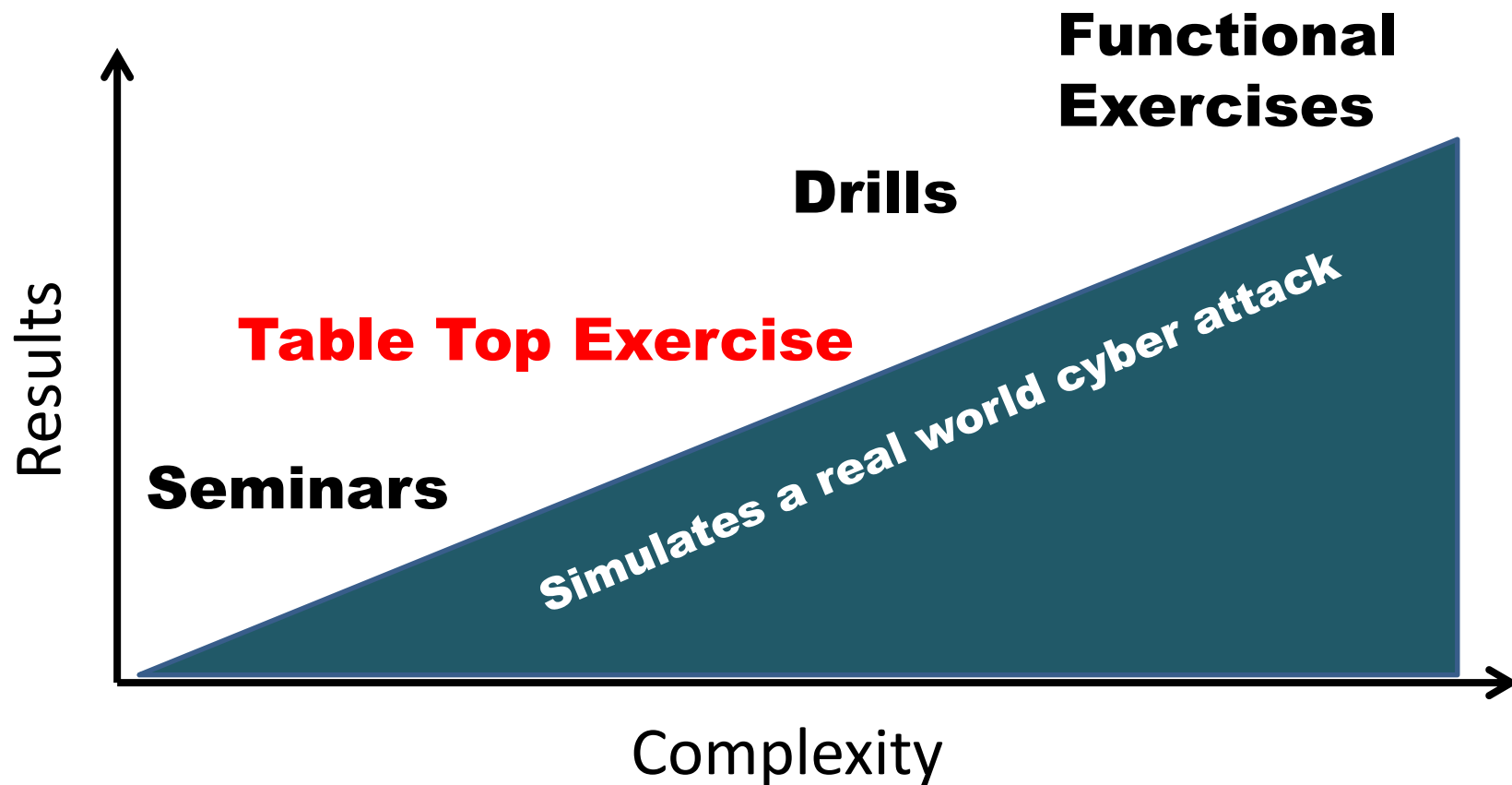


Why train for Incident Response?

- **Enhance** agency Continuity of Operations
- **Minimize** impact on agency Mission Essential Functions
- **Facilitate** returning to normal operations

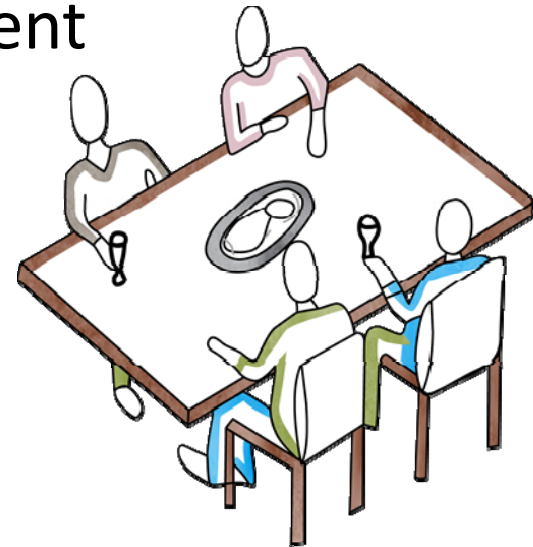


Incident Response Training



What is a Tabletop Exercise?

- Tabletop exercise (TTX)
 - Discussion based session(s)
 - Informal, classroom setting
 - Emphasize roles during an emergency
 - Practice response(s) to an incident
 - Scenarios
 - Injects
 - Procedures
 - Responses



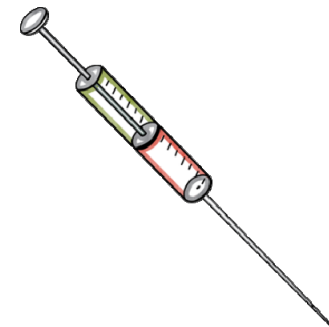
TTX Run Book

- Concept of Operations – Goal, Objectives, Scope
- Coordination Meetings – Concept, Planning
- Training Approach – Seminar, TTX, OpEx
- Objectives and Outcomes
- Scenario and Injects
- Venue
- Communications Plan
- Lessons Learned



Creating TTX Injects

- Scenario based situations requiring a response (deliverable) from TTX participants
- Sample Inject
 - An executive is scheduled for an interview
- Sample Deliverable (Communications Team)
 - Update a list of approved talking points
- Inject deliverables
 - Based on documented procedures
 - Created in advance where possible



TTX Scenario



TTX Scenario - Ransomware

- Criminals targeted information systems
- Ransomware encrypted user files on dozens of systems (laptops, desktops and servers)
- Mission Essential Functions (MEF) disrupted
- \$99,000 ransom is due today
- Ransom is payable in Bitcoin



TTX Injects

General Counsel Team (example)

- The Agency Head asks about Cyber Insurance
- Key elements to address –
 - Does the agency have Cyber Insurance?
 - What does it cover?
 - What is the coverage amount?
 - Is the coverage adequate?
 - Are there “preferred” providers?
 - Will it cover Bitcoin Ransoms?
 - What about TX BCC 521.053?



Team Briefings

- 3 minute discussion of injects
- Relate to real world
- Benefit of documented procedures



IR Program – Assessment

- Define Incident Response
- Establish Governance
- Identify Teams
- Initiate Training
- **Self-Assessment**



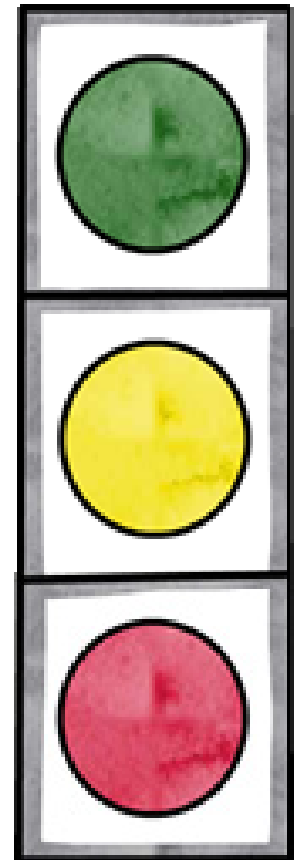
Lessons Learned

- What was supposed to happen?
- What actually happened?
- Why were there differences?
- What worked?
- What didn't?
- Why?



Post-Training Self-Assessment

- T—Trained
 - The team demonstrates proficiency with incident response tasks
- P—Needs practice
 - The team demonstrates difficulty with incident response tasks
- U—Untrained
 - The team cannot demonstrate proficiency with incident response tasks



References

- NIST SP 800-61. (2012, August). *Computer Security Incident Handling Guide Rev 2*. National Institute of Standards and Technology. Washington, DC: Retrieved from <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- NIST SP 800-84. (2006, September). *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*. National Institute of Standards and Technology. Washington, DC: Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf>
- PPD-41. (2016, July 26). *Presidential Policy Directive -- United States Cyber Incident Coordination*. The White House, Office of the Press Secretary. Washington, DC: Retrieved from <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>
- TX DIR(2014, July). *Incident Response Team Redbook*. Texas Department of Information Resources. Austin, TX: Retrieved from <http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template.docx>

Questions



Dave Gray
CyberSecurity Senior Analyst
Texas Comptroller of Public Accounts
www.linkedin.com/in/davidleegray